RSAC 2025 Conference

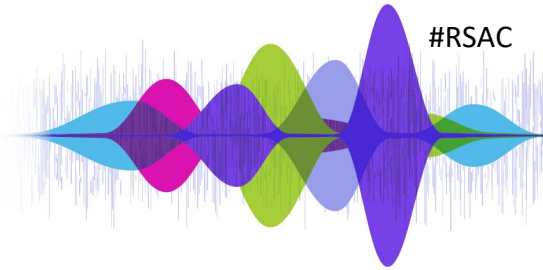
Many Voices.
One Community.

SESSION ID: APP-R03

How to Scale AppSec Without Scaling Security Head Count

Mario Lacroix

Security Delivery Senior Manager
Accenture
https://www.linkedin.com/in/mariolacroix/



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

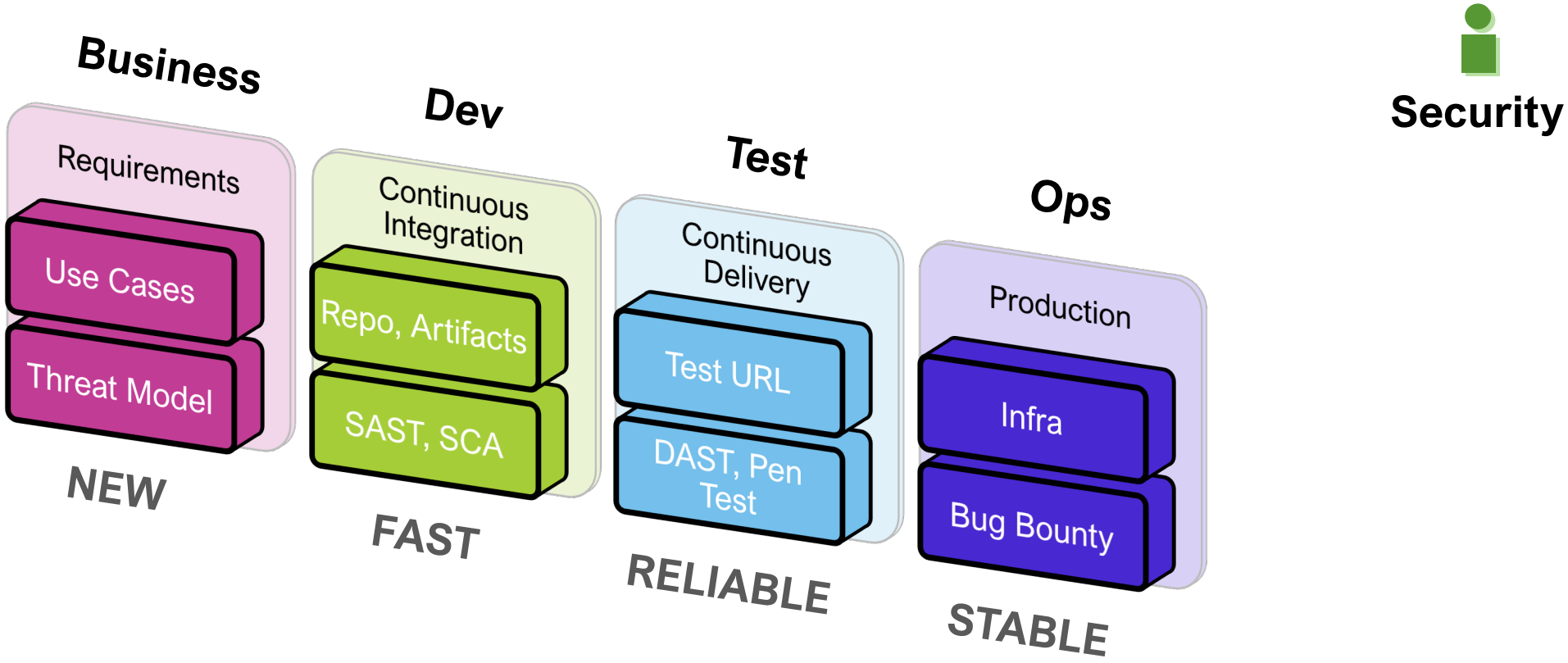
RSAC 2025 Conference

Application Security in 10 Minutes

Why the current approach does not work

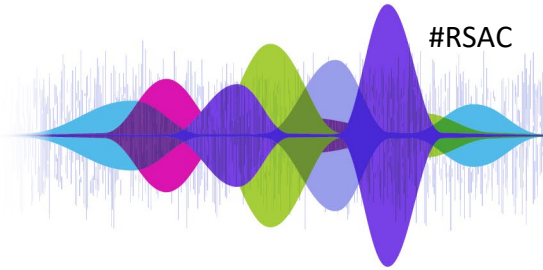
Many Voices.
One Community.

Application Security in 10 minutes



RSAC™ 2025 Conference

The Problem



The Problem

- Tools? what needs to run? What license model to follow?
- CIO/CISO costs calculated based on headcount, managed by business?
- Risk calculation…“Just tell me what is my current risk?”
- Hard to hire and keep security people. “I know what to do… but I don’t have enough hands for all of this”

The REAL Problem

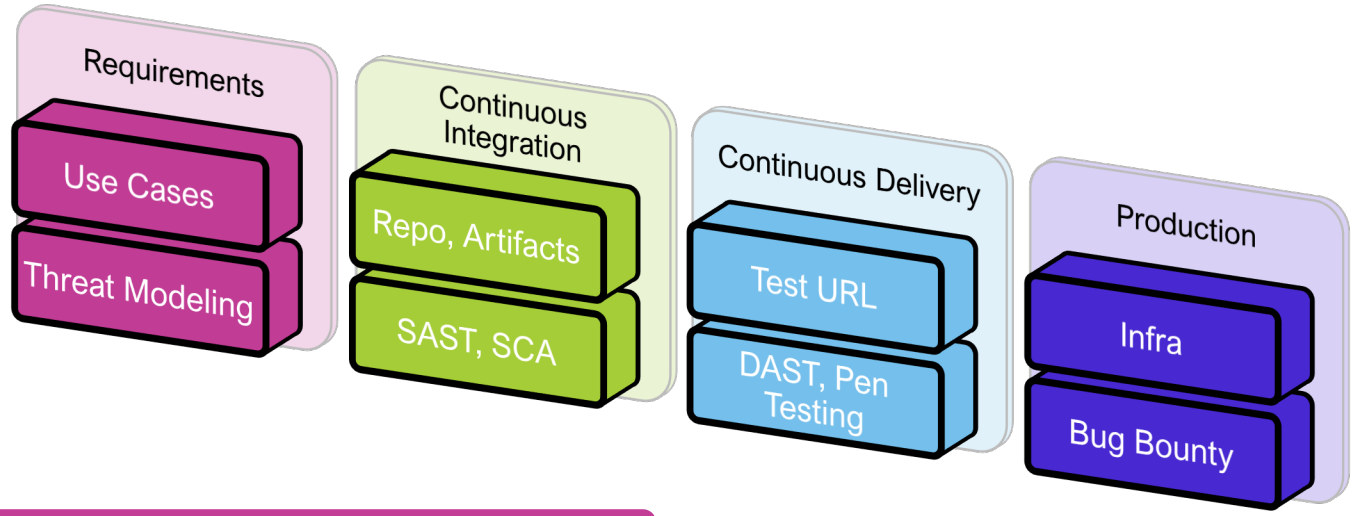
- What needs to be secured? CMDB, portfolio assessment, pipelines, branches, cloud… “shadow digital assets”
- Running the security tools? Schedule, consistency, trouble shooting errors
- DevOps don’t understand what to tackle on all of those big reports? Removing False Positives, prioritizing
- Vulnerability Management: managing tickets, risks

RSAC 2025 Conference

Our Solution

Many Voices.
One Community.

Innovations Embedded into the SDLC



Gating

Enforce policy: No critical vulnerabilities going to production

Power Platform

Power BI tool that correlates risks and drives decision support – also a status reporting window to leadership and Application security posture

ArcBot

AI powered Automation to add security requirements to the application

- Automate integration with SDLC (functional requirements, application information, workflows)
- Interface with application requirements tools (ADO, Jira, etc.)
- Guide developers by adding security requirements

AppSec Advisory Bot

AI powered chatbot talks to developers and guides throughout the security process to:

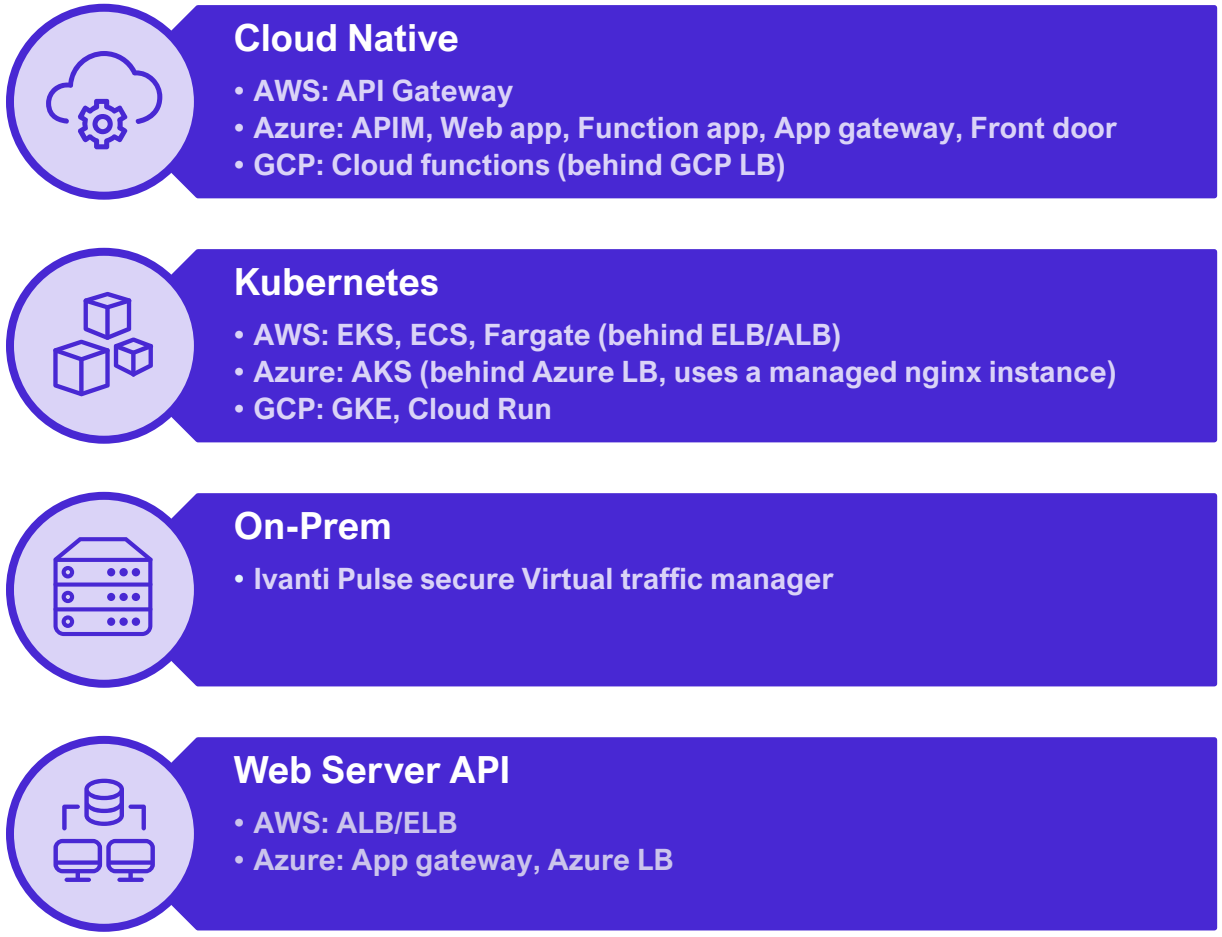
- Automate integration with SDLC (app info, authorization, code repo, pipeline)
- Interface with security scanner outputs (artifact or not)
- Guide developers to perform consistent FPA
- Automate False Positive tag on the systems

PenBot

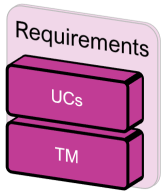
Custom tests at scale for specific tests

Scope – Portfolio and API Discovery

- Process to understand the whole landscape, including current and possible future integration points
- Automated detection using cloud native, commercial and custom tools
- Standardize a process to define contextualization, criticality, data classification, teams, impact, etc.


Cloud Native
• AWS: API Gateway
• Azure: APIM, Web app, Function app, App gateway, Front door
• GCP: Cloud functions (behind GCP LB)
Kubernetes
• AWS: EKS, ECS, Fargate (behind ELB/ALB)
• Azure: AKS (behind Azure LB, uses a managed nginx instance)
• GCP: GKE, Cloud Run
On-Prem
• Ivanti Pulse secure Virtual traffic manager
Web Server API
• AWS: ALB/ELB
• Azure: App gateway, Azure LB

Requirement Gathering - ArcBot

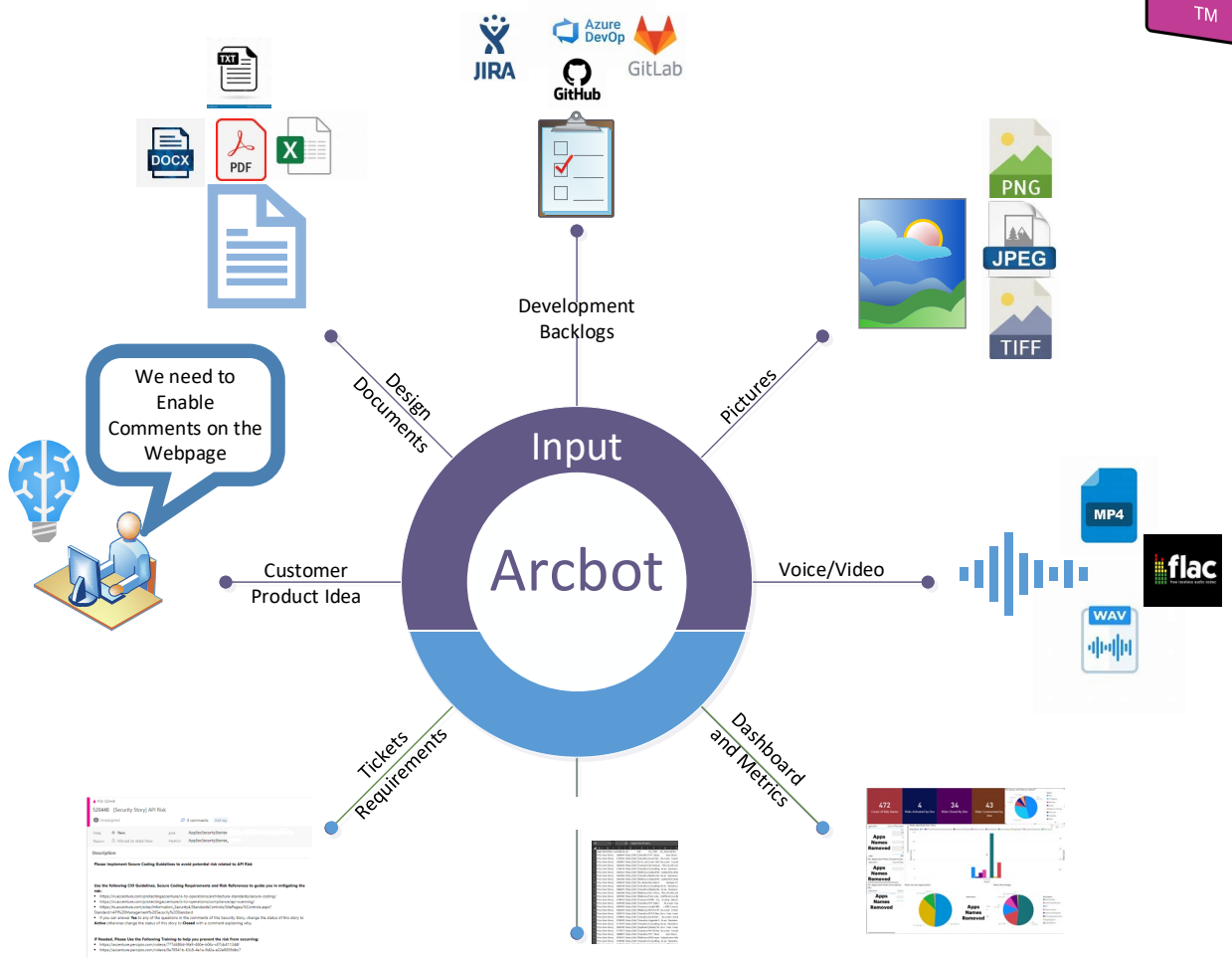


"Translating implicit security risks into explicit requirements."

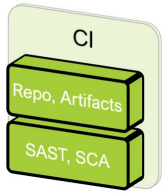
All the value of embedding a dedicated security architect into development teams during design at a fraction of the cost, with no alteration or disruption to the team's staffing model.

ArcBot is a fully automated **AI driven software development tool** that derives security requirements from functional features and interacts with **any desired number of developers at scale** decoupled from security expert headcount.

ArcBot **creates tangible shift left metrics** where developers learn how to make code more secure.



CI – Orchestration and Advisory Bot



Automated Orchestration, Abstraction & Governance

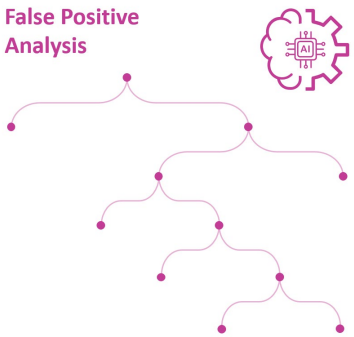
APPLICATION ONBOARDING AT SCALE

Onboard apps **consistently** through tailored **automated workflows** rapidly at massive scale.

AUTOMATED, MEANINGFUL SCANNING

Get meaningful results from properly configured scans. Enable **earlier and deeper insights** through automated **consistent execution**. Works with DevSecOps & Legacy Waterfall.

Security into DevOps Toolbox



FOCUSED, TRIAGED RESULTS

Reduce false positives by 50-80% with automated **upfront filtering and guided decision processes** from decades of false positive analysis (FPA) experience.

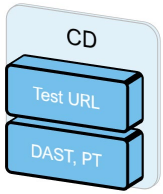
CLEAR, ACTIONABLE REPORTS

Automatically generate **prioritized reports** for consistency, at scale. Out of the box integration with EGRC threat and vulnerability management systems.

REMEDIATION SUPPORT

Provide **remediation guidance** to developers and **mitigation guidance** to Ops and app support teams to accelerate remediation.

CD – PenBot



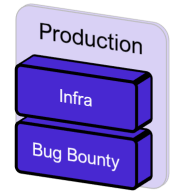
Challenges

- How to test that a given finding exists only once, versus in multiple locations throughout the environment?
- How to test that preventative controls are being followed?
- How to prevent the reoccurrence of specific types of vulnerabilities?
- How can business logic be tested when it extends beyond a “single application” (e.g., Identity services)?

Solution

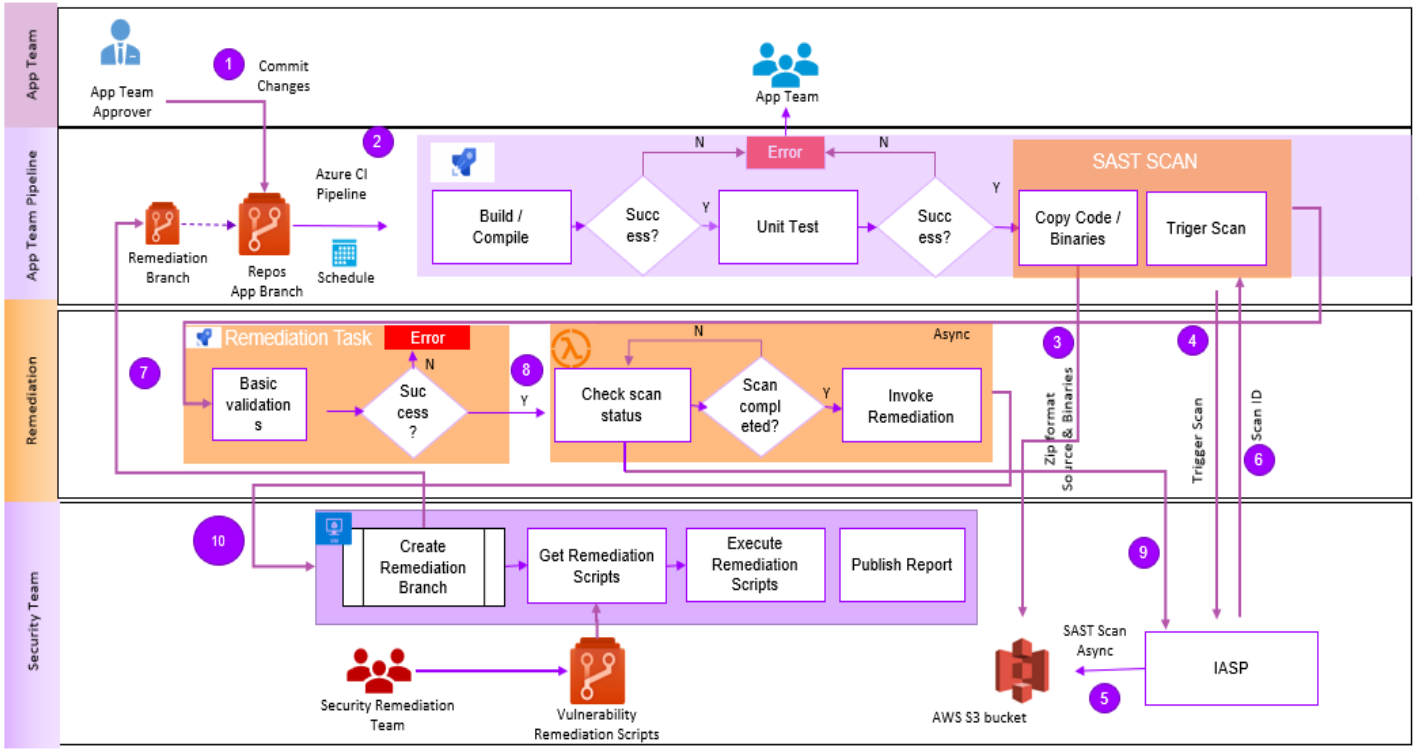
- Custom automate other security tools such as:
  - DNS Queries
  - DAST output
  - Manual crawling
- Accuracy
  - Defining evaluations collaboratively with enterprise architects decreases the rate of inaccurate findings (90+% accuracy)
  - Automations can be tuned to facilitate enhanced accuracy

Auto Remediation and Mitigation



Turning SAST Findings into Secure Code

- Ingest Static Application Security Testing (SAST) scan results, clones the branch, and remediates vulnerabilities found. Developer can accept or reject.
- Java and C# support.
- Can be integrated seamlessly into CI/CD pipelines through APIs.
- Asynchronous process, with no disruption to regular work activities.



RSAC 2025 Conference

AppSec Advisory Chatbot

Demo

Many Voices.
One Community.

Chatbot Groundwork: Ground Truth

Documenting Knowledge

- Interview SMEs and SMAs
- Multi discipline team
- Tested, validated, adopted by MSS
- We documented things like: How to validate false positives, how to remediate, how to mitigate, mapped impacts, multiple layers
- Constant improvements

Enhancing DevOps

- Standardized process
- DevOps don’t have time (nor want) to learn about security
- Scanner tools are too generic “To fix this, read the OWASP cheat sheet”
- Adding security as part of the DevOps toolbox

AppSec Advisory Chatbot Business Value

01

DevOps Security Autonomy

The project adds to the DevOps toolbox which is part of the demanded security tools and workflows that bring autonomy to the development teams to analyze detected security issues.

Conversations with the bot improve the developer's security knowledge on the vulnerability and how to fix it.

02

Optimized Developer Remediation Time

Automations to help removing non-relevant tasks and help the DevOps teams prioritize what needs to be fixed. No need to use other processes to request exceptions anymore!

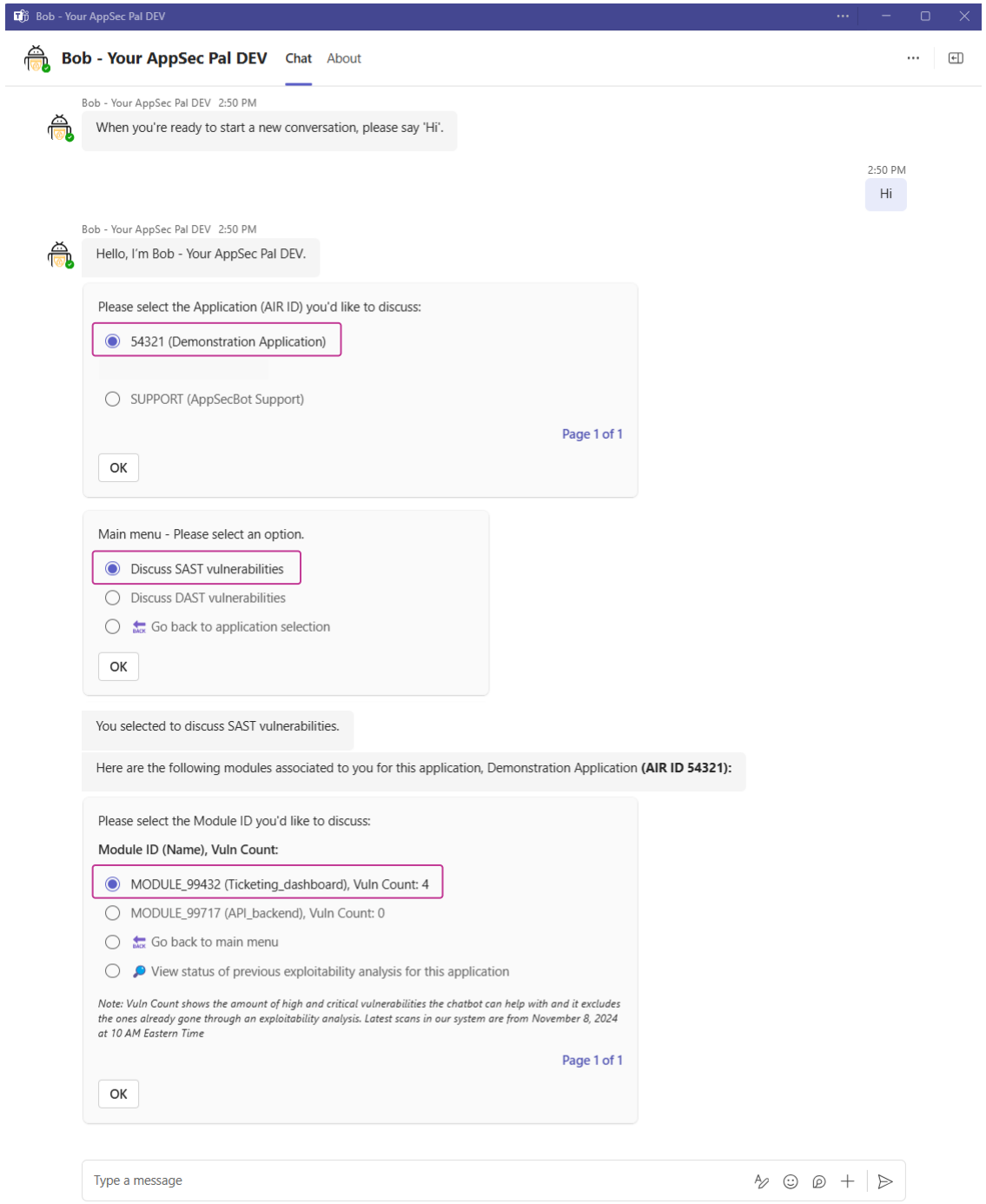
03

Compliance Improvements

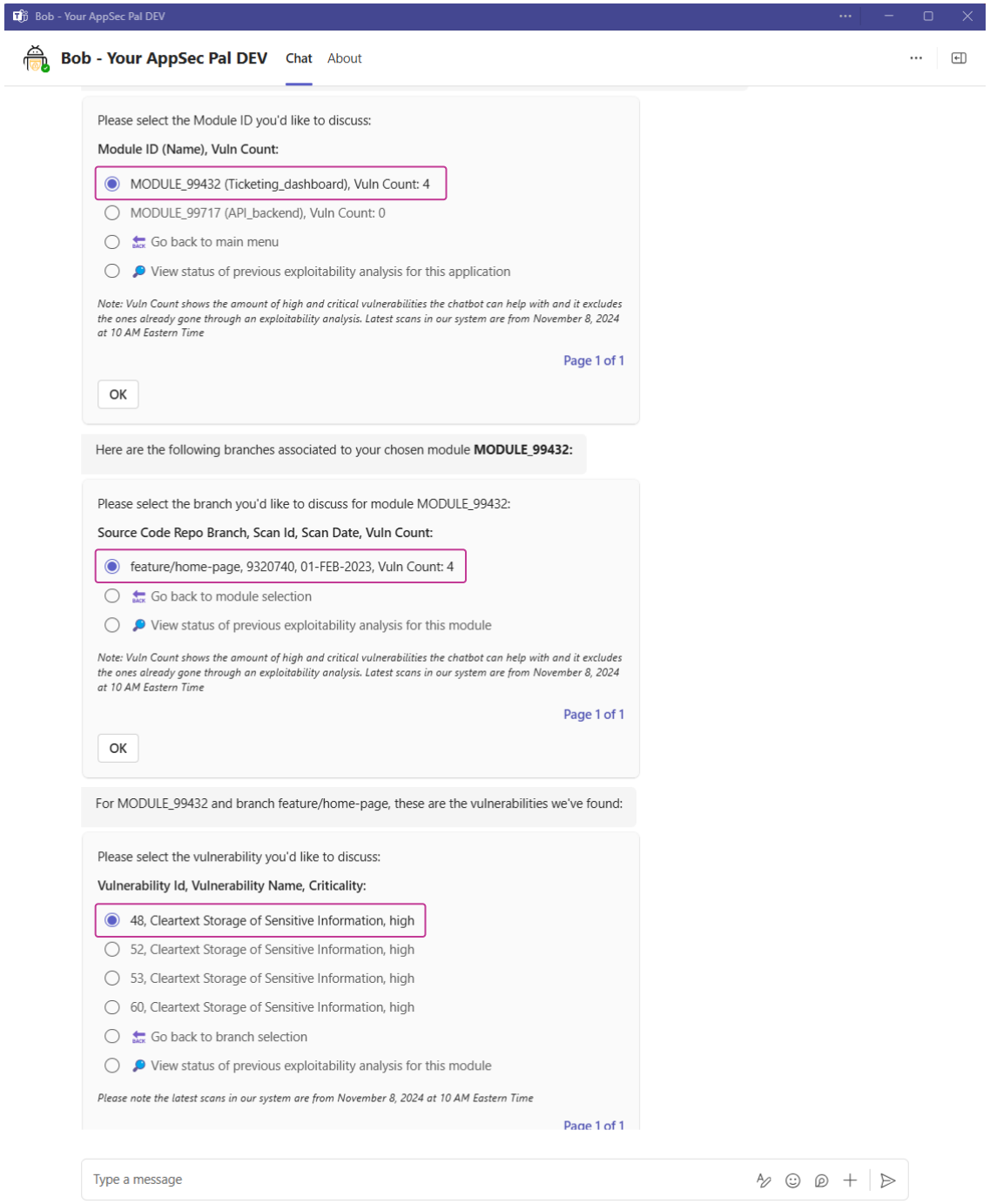
The conversation itself works as documentation about why a vulnerability is non-exploitable (the request is automatically closed) OR exploitable (the developer can work on it following the proper target times).

Chatbot Demo

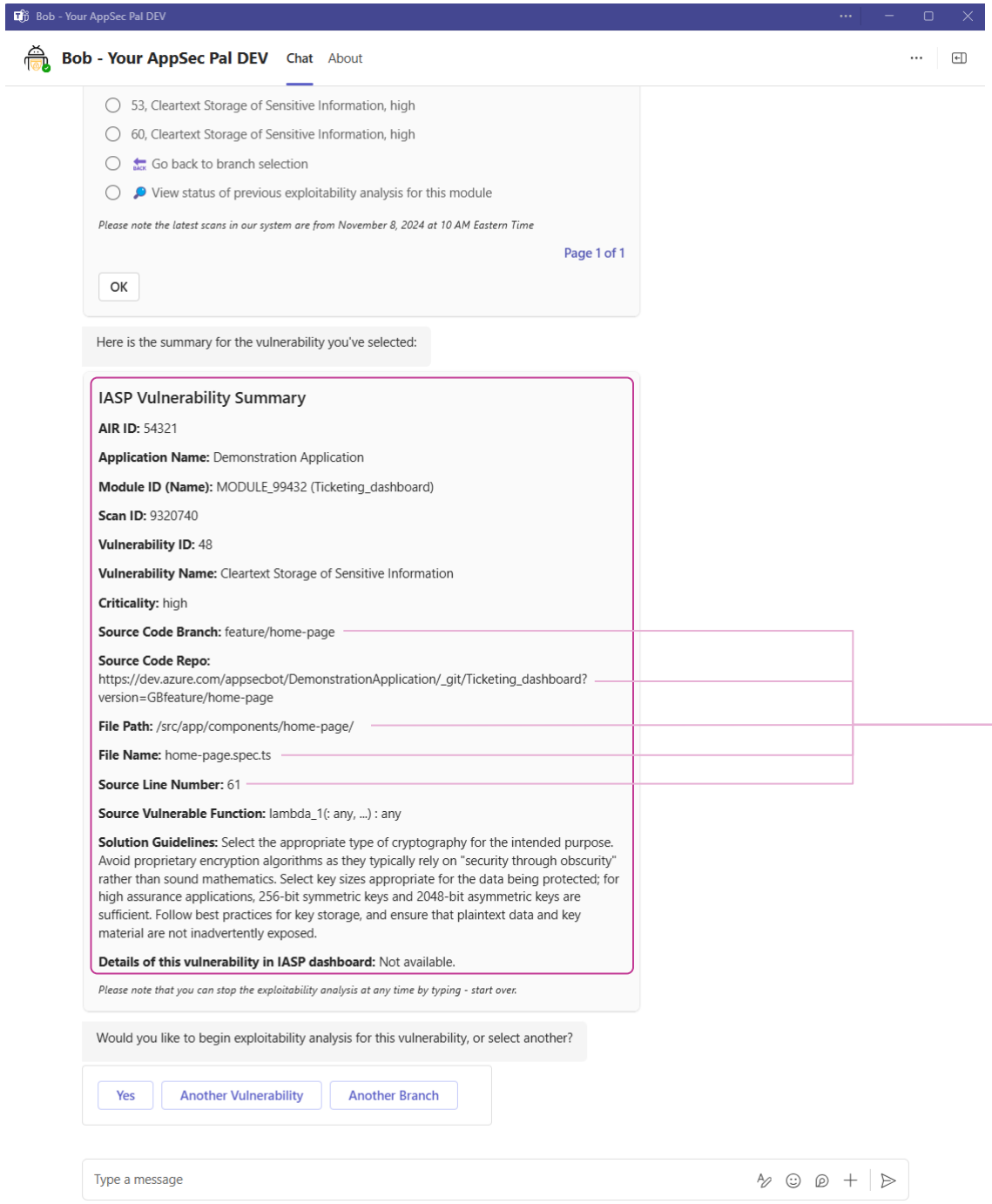
Application & Module (Repo) Selection


Bot - Your AppSec Pal DEV
Bob - Your AppSec Pal DEV
Chat
About
Bob - Your AppSec Pal DEV 2:50 PM
When you're ready to start a new conversation, please say 'Hi'.
2:50 PM
Hi
Bob - Your AppSec Pal DEV 2:50 PM
Hello, I'm Bob - Your AppSec Pal DEV.
Please select the Application (AIR ID) you'd like to discuss:
54321 (Demonstration Application)
SUPPORT (AppSecBot Support)
Page 1 of 1
OK
Main menu - Please select an option.
Discuss SAST vulnerabilities
Discuss DAST vulnerabilities
Go back to application selection
OK
You selected to discuss SAST vulnerabilities.
Here are the following modules associated to you for this application, Demonstration Application (AIR ID 54321):
Please select the Module ID you'd like to discuss:
Module ID (Name), Vuln Count:
MODULE_99432 (Ticketing_dashboard), Vuln Count: 4
MODULE_99717 (API_backend), Vuln Count: 0
Go back to main menu
View status of previous exploitability analysis for this application
Note: Vuln Count shows the amount of high and critical vulnerabilities the chatbot can help with and it excludes the ones already gone through an exploitability analysis. Latest scans in our system are from November 8, 2024 at 10 AM Eastern Time
Page 1 of 1
OK
Type a message

Branch & Vulnerability Selection


Bob - Your AppSec Pal DEV
Bob - Your AppSec Pal DEV
Chat
About
Please select the Module ID you'd like to discuss:
Module ID (Name), Vuln Count:
MODULE_99432 (Ticketing_dashboard), Vuln Count: 4
MODULE_99717 (API_backend), Vuln Count: 0
Go back to main menu
View status of previous exploitability analysis for this application
Note: Vuln Count shows the amount of high and critical vulnerabilities the chatbot can help with and it excludes the ones already gone through an exploitability analysis. Latest scans in our system are from November 8, 2024 at 10 AM Eastern Time
Page 1 of 1
OK
Here are the following branches associated to your chosen module MODULE_99432:
Please select the branch you'd like to discuss for module MODULE_99432:
Source Code Repo Branch, Scan Id, Scan Date, Vuln Count:
feature/home-page, 9320740, 01-FEB-2023, Vuln Count: 4
Go back to module selection
View status of previous exploitability analysis for this module
Note: Vuln Count shows the amount of high and critical vulnerabilities the chatbot can help with and it excludes the ones already gone through an exploitability analysis. Latest scans in our system are from November 8, 2024 at 10 AM Eastern Time
Page 1 of 1
OK
For MODULE_99432 and branch feature/home-page, these are the vulnerabilities we've found:
Please select the vulnerability you'd like to discuss:
Vulnerability Id, Vulnerability Name, Criticality:
48, Cleartext Storage of Sensitive Information, high
52, Cleartext Storage of Sensitive Information, high
53, Cleartext Storage of Sensitive Information, high
60, Cleartext Storage of Sensitive Information, high
Go back to branch selection
View status of previous exploitability analysis for this module
Please note the latest scans in our system are from November 8, 2024 at 10 AM Eastern Time
Page 1 of 1
Type a message

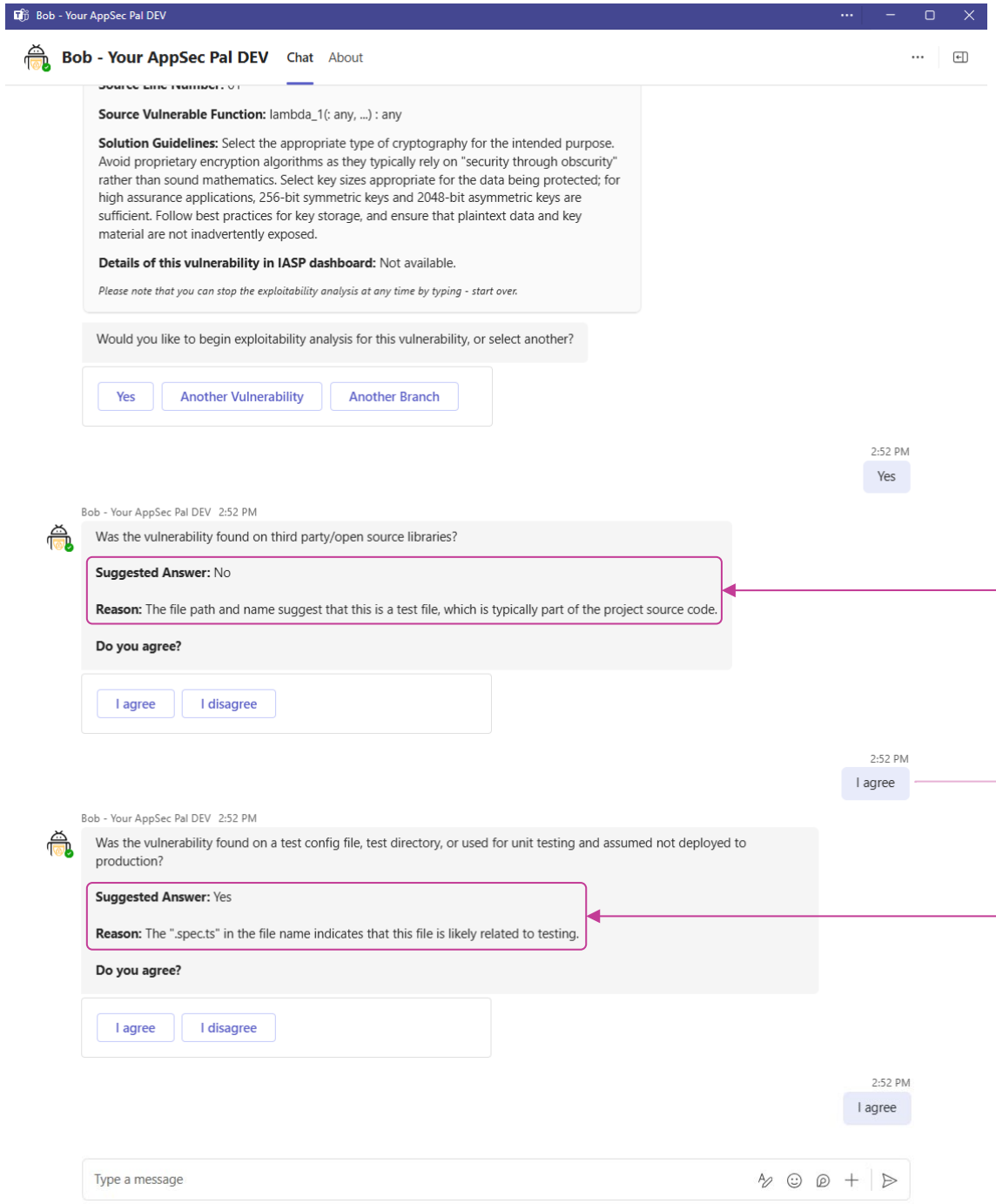
Vulnerability Summary

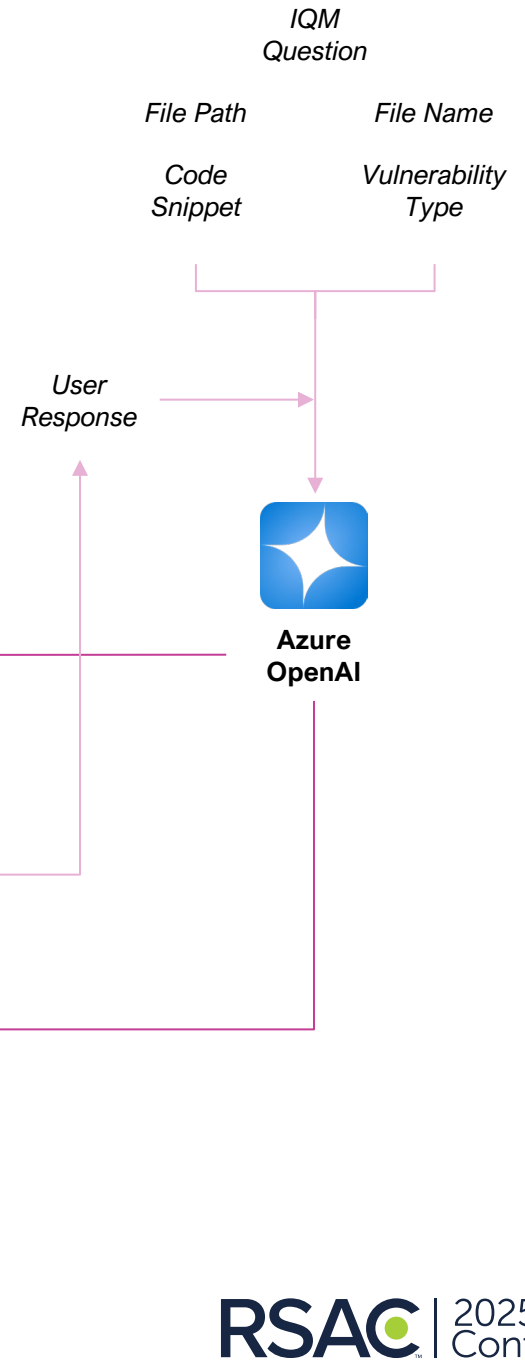

Bob - Your AppSec Pal DEV
Bob - Your AppSec Pal DEV
Chat
About
53, Cleartext Storage of Sensitive Information, high
60, Cleartext Storage of Sensitive Information, high
Go back to branch selection
View status of previous exploitability analysis for this module
Please note the latest scans in our system are from November 8, 2024 at 10 AM Eastern Time
Page 1 of 1
OK
Here is the summary for the vulnerability you've selected:
IASP Vulnerability Summary
AIR ID: 54321
Application Name: Demonstration Application
Module ID (Name): MODULE_99432 (Ticketing_dashboard)
Scan ID: 9320740
Vulnerability ID: 48
Vulnerability Name: Cleartext Storage of Sensitive Information
Criticality: high
Source Code Branch: feature/home-page
Source Code Repo: https://dev.azure.com/appsecbot/DemonstrationApplication/_git/Ticketing_dashboard?version=GBfeature/home-page
File Path: /src/app/components/home-page/
File Name: home-page.spec.ts
Source Line Number: 61
Source Vulnerable Function: lambda_1(: any, ...) : any
Solution Guidelines: Select the appropriate type of cryptography for the intended purpose. Avoid proprietary encryption algorithms as they typically rely on "security through obscurity" rather than sound mathematics. Select key sizes appropriate for the data being protected; for high assurance applications, 256-bit symmetric keys and 2048-bit asymmetric keys are sufficient. Follow best practices for key storage, and ensure that plaintext data and key material are not inadvertently exposed.
Details of this vulnerability in IASP dashboard: Not available.
Please note that you can stop the exploitability analysis at any time by typing - start over.
Would you like to begin exploitability analysis for this vulnerability, or select another?
Yes
Another Vulnerability
Another Branch
Type a message

Azure DevOps Repository

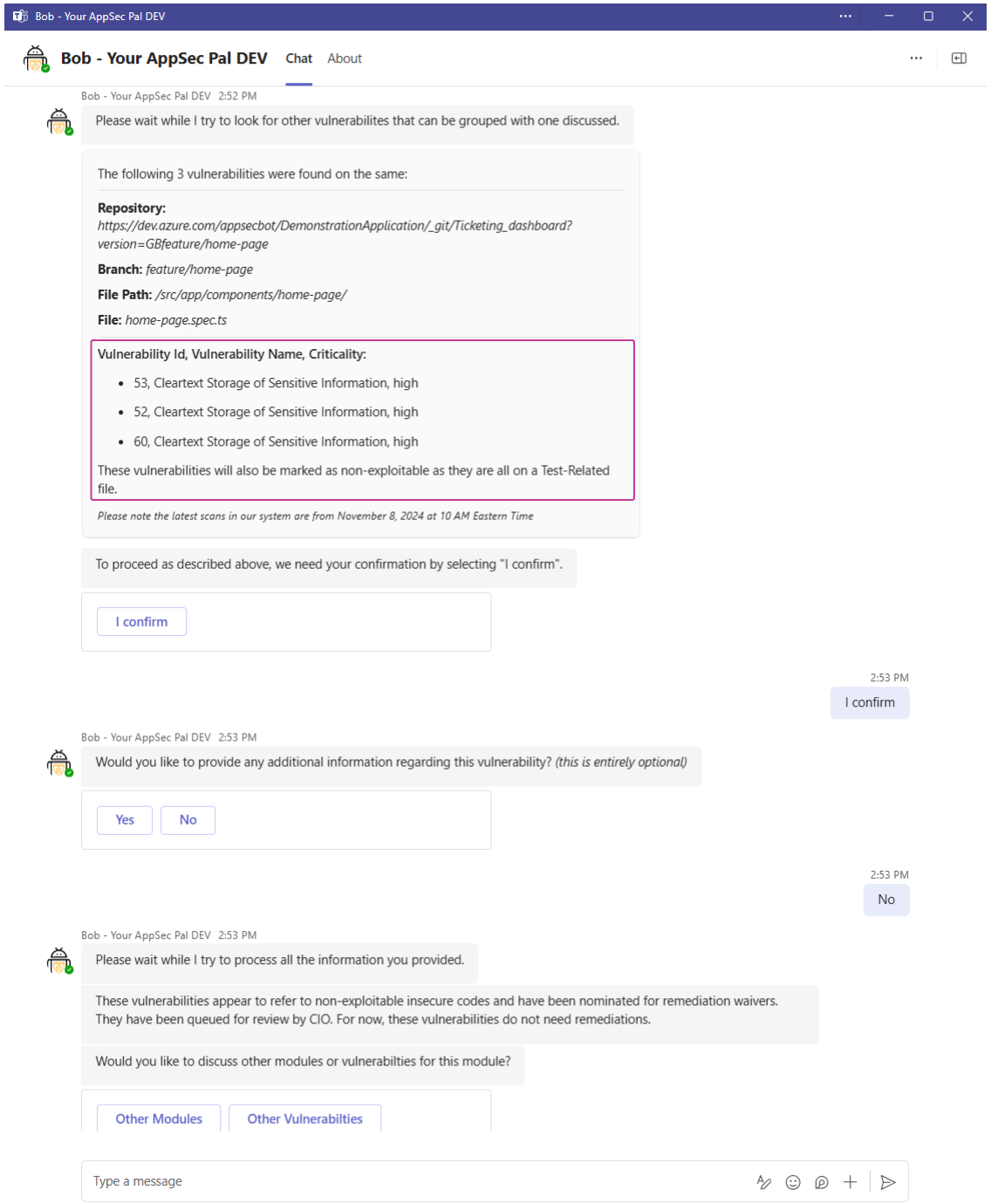
Code Snippet

Exploitability (False Positive) Analysis


Bob - Your AppSec Pal DEV
Bob - Your AppSec Pal DEV
Chat
About
Source Vulnerable Function: lambda_1(: any, ...) : any
Solution Guidelines: Select the appropriate type of cryptography for the intended purpose. Avoid proprietary encryption algorithms as they typically rely on "security through obscurity" rather than sound mathematics. Select key sizes appropriate for the data being protected; for high assurance applications, 256-bit symmetric keys and 2048-bit asymmetric keys are sufficient. Follow best practices for key storage, and ensure that plaintext data and key material are not inadvertently exposed.
Details of this vulnerability in IASP dashboard: Not available.
Please note that you can stop the exploitability analysis at any time by typing - start over.
Would you like to begin exploitability analysis for this vulnerability, or select another?
Yes
Another Vulnerability
Another Branch
2:52 PM
Yes
Bob - Your AppSec Pal DEV 2:52 PM
Was the vulnerability found on third party/open source libraries?
Suggested Answer: No
Reason: The file path and name suggest that this is a test file, which is typically part of the project source code.
Do you agree?
I agree
I disagree
2:52 PM
I agree
Bob - Your AppSec Pal DEV 2:52 PM
Was the vulnerability found on a test config file, test directory, or used for unit testing and assumed not deployed to production?
Suggested Answer: Yes
Reason: The ".spec.ts" in the file name indicates that this file is likely related to testing.
Do you agree?
I agree
I disagree
2:52 PM
I agree
Type a message



Grouping Similar Vulnerabilities


Bob - Your AppSec Pal DEV
Bob - Your AppSec Pal DEV
Chat
About
Bob - Your AppSec Pal DEV 2:52 PM
Please wait while I try to look for other vulnerabilites that can be grouped with one discussed.
The following 3 vulnerabilities were found on the same:
Repository:
https://dev.azure.com/appsecbot/DemonstrationApplication/_git/Ticketing_dashboard?version=GBfeature/home-page
Branch: feature/home-page
File Path: /src/app/components/home-page/
File: home-page.spec.ts
Vulnerability Id, Vulnerability Name, Criticality:
53, Cleartext Storage of Sensitive Information, high
52, Cleartext Storage of Sensitive Information, high
60, Cleartext Storage of Sensitive Information, high
These vulnerabilities will also be marked as non-exploitable as they are all on a Test-Related file.
Please note the latest scans in our system are from November 8, 2024 at 10 AM Eastern Time
To proceed as described above, we need your confirmation by selecting "I confirm".
I confirm
2:53 PM
I confirm
Bob - Your AppSec Pal DEV 2:53 PM
Would you like to provide any additional information regarding this vulnerability? (this is entirely optional)
Yes
No
2:53 PM
No
Bob - Your AppSec Pal DEV 2:53 PM
Please wait while I try to process all the information you provided.
These vulnerabilities appear to refer to non-exploitable insecure codes and have been nominated for remediation waivers. They have been queued for review by CIO. For now, these vulnerabilities do not need remediations.
Would you like to discuss other modules or vulnerabilties for this module?
Other Modules
Other Vulnerabilties
Type a message

RSAC 2025 Conference

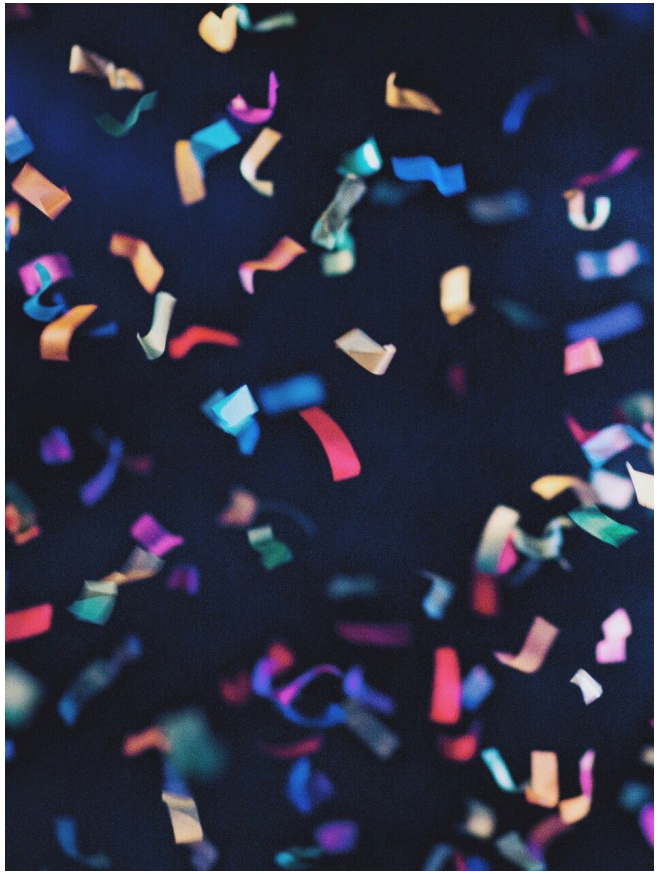
Outcomes

How can you build it?

- Document the process the security team is performing IN DETAIL, them simplify it to be used by junior developers.
- Build integrations of ALL security scanners in use, optimize it, orchestrate it, automate workflows, and concentrate all in one place.
  - Current ASPM tools will not solve all of this. Be ready to build some integrations and automations yourself
  - Normalize the reports from all security tools… yeah, they are all different…
- Assemble a team of developers and security people, document the ACTUAL requirements they expect to be covered, build chat workflows, optimize the conversations and automate!
- Get continuous feedback from developers. Understand the metrics properly (zero target: you want zero vulnerabilities open so people not using bots)

A Few Metrics After 1 Year

- ArcBot: 70k security review, 700+ applications, small operational team. 12x fewer vulnerabilities generated across applications at the end of first year.*
- AppSec Advisory Bot: Empowerment of developers and true shift left. Reduced scanning cost and effort by ~40%. On the first year, developer-performed FPA accuracy went from 10% to nearly 100%. Faster overall process and cycle.
- Auto-R: 21.000+ fixes proposed, reduced 9Y of labor cost
- PenBot: More than 80 person-years of testing effort with a few offshore low-cost operators. After remediating findings, saw a >95% decrease in volume of rigorous 3rd-party penetration test findings.



*Based on an analysis and scope of applications from previous clients

RSAC™ 2025 Conference

Apply

Many Voices.
One Community.

You Can Apply AI and Automations!

- Collaborative approach!
- Empower your DevOps teams to become security champions, adding the security tools into the DevOps toolbox.
- Choose the right mix of AI, ML, RAG and Automations to guide, and help making Dev & Ops life easier.
- Instrumentalize your internal knowledge and get crowd help to constantly evolve it.
- It’s not easy to find everything you need to secure. “Whatever you have now is not complete” mindset. DevOps can help you find it.
- Challenge yourself to think in a different way.

RSAC 2025 Conference

Many Voices.
One Community.

Thank you

For more information:

www.accenture.com/us-en/services/security/application-security